(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－513491
（P2002－513491A）
(43)公表日　平成14年５月８日(2002.5.8)

(51)Int.Cl.'	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	１１２	Ｇ０６Ｆ　17/60	１１２Ｃ
Ｇ０７Ｂ　17/00		Ｇ０７Ｂ　17/00	

審査請求　未請求　予備審査請求　有　（全 27 頁）

(21)出願番号　特願平11－503266
(86)(22)出願日　平成10年６月12日(1998.6.12)
(85)翻訳文提出日　平成11年２月12日(1999.2.12)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／１２２７６
(87)国際公開番号　ＷＯ９８／５７３０４
(87)国際公開日　平成10年12月17日(1998.12.17)
(31)優先権主張番号　６０／０４９，５１８
(32)優先日　平成９年６月12日(1997.6.12)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ピットニイ　ボウズ　インコーポレイテッド
アメリカ合衆国　コネチカット州　06926
スタムフォード　ワン　エルムクロフト　ロード（番地なし）
(72)発明者　コーデリー　ロバート　エイ
アメリカ合衆国　コネチカット州　06811
ダンバリー　ジャネット　ストリート　11－１－２
(72)発明者　デポリット　フランク　エム
アメリカ合衆国　コネチカット州　06418
デルビー　コモドア　コモンズ　47
(74)代理人　弁理士　中村　稔　（外６名）

最終頁に続く

(54)【発明の名称】　安全なデジタル署名デバイスを有する仮想郵便料金メーター

(57)【要約】
郵便料金支払い証明のシステム(10)と方法のデータセンター(3)は、内部に複数のメーター記録(64)を有するデータベース(36)を備える。各メーター記録(64)は、郵便料金支払い証明の要求を許可された複数の遠隔ユーザーデバイス(20,22)に割り当てられる個々のメーターの口座に対応するメーター情報を含む。データセンター(30)で、郵便料金の要求(100)を受取ると、データセンター(30)の安全な双対プロセッサーデバイス(44)が、適切なメーター記録(64)を得て、メーター記録(64)の署名を検証し(205,210)、メーター記録(64)のフレッシュネスデータを安全デバイス(44)のフレッシュネスデータと比較することにより、メーター記録(64)の承認を検証する。検証されれば、安全デバイス(44)は、証明される郵便料金価額を会計し(130)、郵便料金支払い証明を生成し(130)、メーター記録(64)内のフレッシュネスデータを含むメーター情報を更新する(130)。安全デバイス(44)は、更新したメーター情報に署名し、メーター記録に署名を記憶する(64,135,140)。安全デバイス(44)は、更新したメーター記録(64)をデータベースに戻す(36,135,140)。

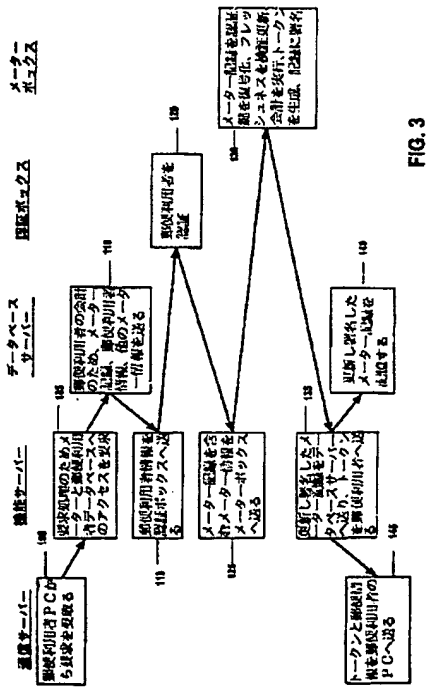

FIG. 3

【特許請求の範囲】

1．安全な郵便料金分配システムにおいて、

複数の遠隔ユーザーデバイスからの郵便証印要求に応答して、郵便証印を分配するデータセンターを備え、前記データセンターは、

ユーザー情報と、前記複数の遠隔ユーザーデバイスに割り当てられる各メーターの口座のメーター情報を含むデータ記録を記憶するデータベース手段、

前記複数の遠隔ユーザーデバイスから郵便料金証明の要求を受取る手段、

前記ユーザー情報と、郵便料金証明の要求を開始する前記遠隔ユーザーデバイスのメーターの口座に対応する前記メーター情報を使用して、郵便料金証明の各要求を認証する手段、及び、

プロセッサーとメモリーを含む少なくとも1つの第1安全デバイスを含む、要求された郵便料金証明を分配する手段を備え、

前記第1安全デバイスは、前記データベース手段から前記メーター情報を得て、前記メーター情報の認証を検証し、要求された郵便料金証明を生成し、前記メーター情報を更新し、更新されたメーター情報にデジタル署名し、署名し更新されたメーター情報を前記データベース手段に戻すことを特徴とするシステム。

2．前記データベース手段は、メーター記録のデータベースを含み、各メーター記録は、前記複数の遠隔ユーザーデバイスのためのメーターの口座の1つに対応するメーター情報と、前記メーター情報の署名を含む請求の範囲第1項に記載したシステム。

3．前記メーター情報は、昇順及び降順レジスターと、暗号化トークン鍵と、フレッシュネスデータとを含む請求の範囲第2項に記載したシステム。

4．前記フレッシュネスデータは、前記安全デバイスで処理される郵便証明取引の数に対応する記録更新カウンターを備える請求の範囲第3項に記載したシステム。

5．前記第1安全デバイスは、第1、第2暗号鍵を記憶する手段を含み、前記第1鍵は、各メーター記録の署名を検証し、また各メーター記録を前記データベ

ス手段に戻す前に更新したメーター情報に署名するため使用され、前記第２鍵は、前記メーター記録の暗号化されたトークン鍵を復号化するため使用され、前記安全デバイスは、要求された郵便料金証明を生成するのにトークン鍵を使用する請求の範囲第２項に記載したシステム。

６．機能サーバーが、前記通信サーバーにより受取られた各要求を処理し、前記データベースサーバーから適当なユーザー情報とメーター情報を得て、前記ユーザー情報とメーター情報を前記認証手段と分配手段とに送る請求の範囲第５項に記載したシステム。

７．前記認証手段は、プロセッサーを含む第２安全ボックスと、メモリーと、第３暗号鍵を記憶する手段とを含み、前記第３鍵は処理されるメーターの口座の前記ユーザー情報と対応する署名を検証するため使用される請求の範囲第１項に記載したシステム。

８．前記認証手段と前記分配手段により使用される暗号鍵を生成し保持する鍵管理システムサーバーを備える請求の範囲第７項に記載したシステム。

９．前記受取る手段は通信サーバーを備え、前記データベース手段は、それぞれ前記データセンターにあるデータベースサーバーを備える請求の範囲第１項に記載したシステム。

10．郵便料金支払証明方法において、

郵便料金支払い証明を要求することを認証された複数の遠隔ユーザーデバイスの各々に割り当てられたメーターの口座に対応するメーター情報を含む複数のメーター記録を提供し、

前記複数のメーター記録をデータセンターのデータベースに記憶し、

前記データセンターが郵便料金支払い証明の要求を受取るとき、第１メーター記録を得て、

前記第１メーター記録の署名を検証することにより、前記第１メーター記録の認証を検証し、

証明された郵便料金の価額を会計し、

郵便料金支払い証明としてデジタルトークンを生成し、

前記第１メーター記録の前記メーター情報を更新し、

前記第１メーター記録の署名を更新するため、更新されたメーター情報に署名し、

前記第１メーター記録を前記データベースに戻す、

ステップを備えることを特徴とする方法。

11. 前記得て、検証し、会計し、生成し、更新し、署名し、戻すステップは、安全デバイス内で実行される請求の範囲第１０項に記載した方法。

12. 前記第１メーター記録の認証を検証するステップは、前記第１メーター記録内のフレッシュネスデータを前記安全デバイスに記憶したフレッシュネスデータと比較するステップを備える請求の範囲第１１項に記載した方法。

13. 前記前記メーター情報を更新するステップは、前記安全デバイスと前記第１メーター記録に記憶したフレッシュネスデータを更新するステップを備える請求の範囲第１１項に記載した方法。

【発明の詳細な説明】

安全なデジタル署名デバイスを有する仮想郵便料金メーター

本出願は、1997年６月13日出願で、本発明の譲受人に譲受けられた米国仮特許出願第60/049,518号の一部継続出願である。

技術分野

本発明は、一般にオープンシステムにおいて、郵便料金支払いを証明する郵便料金メーターシステムと方法に関し、より詳しくは、仮想メーターの構成で郵便料金支払いを証明する郵便料金メーターシステムと方法に関する。

関連出願

本発明は、次の米国特許出願(代理人文書番号E-731, E-733, E-734, E-735, E-736)に関連し、これらは全て共に出願され、本発明の譲受人に譲受された。これらの出願の全てをここに参照する。

背景技術

郵便料金支払いを証明する証印の一部として郵便物上に印刷される暗号化情報を用いる郵便料金メーターシステムが発展してきた。暗号情報は、郵便物の郵便価額、及び郵便物及び証印を印刷する郵便料金メーターに関する他の郵便データを含む。暗号化された情報は、一般にデジタルトークン又はデジタル署名といわれ、郵便物の上に印刷された郵便価額を含む情報の完全さを認証して保護し、後に郵便料金支払いを確認できる。デジタルトークンは郵便料金支払いの証明に関する暗号情報を組み込んでいるので証印に印刷された情報を改変すると、標準の検証手順で検知することができる。このような証印を生成し印刷するシステムの例は、本発明の譲受人に譲受けられた米国特許第4,725,718号、第4,757,537号、第4,775,246号、4,873,645号に記述されている。

現在、クローズドシステムとオープンシステムの２つの郵便料金メーターデバイス種類がある。クローズドシステムでは、システムの機能は、メーターの活動専用である。クローズドシステムのメーターデバイスの例は、ここでは郵便料金証明デバイスとも言うが、従来のデジタルとアナログ(機械的と電気的)郵便料金

メーターを備え、専用プリンターがメーター即ち会計機能に安全保護されて結合

している。クローズドシステムでは、一般にプリンターはメーターに安全保護されて結合し、メーター専用であり、郵便料金の証明を印刷すれば、必ず郵便料金証明の会計が行われる。オープンシステムでは、プリンターはメーターの活動に専用ではなく、システムの機能は、メーターの活動に加えて複数の異なる使用ができる。オープンシステムのメーターデバイスの例は、単一／複数タスクのオペレーティングシステム、複数ユーザーのアプリケーション、デジタルプリンターを有するパーソナルコンピュータ（ＰＣ）ベースのデバイスである。オープンシステムのメーターデバイスは、安全な会計モジュールに安全保護されないで結合された非専用プリンターを有する郵便料金証明デバイスである。専用でないプリンターで印刷されたオープンシステムの証印は、郵便物上に印刷された郵便料金の暗号化した証明に受信人情報を含ませることにより、後で検証できるようにして安全保護される。本発明の譲受人に譲受けられた米国特許第4,725,718号、第4,831,555号を参照されたい。

米国郵政公社（ＵＳＰＳ）は、情報ベース証印プログラム（ＩＢＩＰ）を提案した。これは、分配された信頼されるシステムであり、情報ベースの証印という新しい郵便料金支払い証明を使用して現存する郵便料金メーターを改装し、増大させる。このプログラムは、デジタル署名技術によりたのみ、出所を認証でき内容を改変することができない証印を各封筒に作成する。ＩＢＩＰは、一般に郵便料金メーターが郵便物上に証印を印刷する現在の方法に加えて、郵便料金に適用する新しい方法をサポートすることが期待される。ＩＢＩＰは、大きく高密度の２次元（２Ｄ）バーコードを郵便物上に印刷することを要する。２Ｄバーコードは、情報を暗号化し、デジタル署名される。

ＵＳＰＳは、ＩＢＩＰの仕様書案を公表した。1996年６月13日に発表され1997年７月23日に改定された情報ベースの証印プログラム（ＩＢＩＰ）証印仕様書（ＩＢＩＰ証印仕様書）は、ＩＢＩＰを使用して作成された郵便に適用される新しい証印についての要求案を明記する。1996年６月13日に発表され1997年７月23日に改定された情報ベースの証印プログラム郵便セキュリティデバイス仕様書（ＩＢＩＰ　ＰＳＤ仕様書）は、郵便セキュリティデバイス（ＰＳＤ）の要求につ

いての提案を明記する。ここに、ＰＳＤとは、内部に記憶した郵便価額を分配し会計する安全なプロセッサーベースの会計デバイスであり、ＩＢＩＰを使用して処理される郵便に適用される新しい「情報ベースの」郵便料金ポストマーク即ち証印の作成を支援する。1996年10月９日に発表された情報ベース証印プログラムホストシステム仕様書は、ＩＢＩＰのホストシステムの要素への要求案についての明記する(ＩＢＩＰホスト仕様書)。ＩＢＩＰは、インターフェースするユーザー、プログラムのシステム要素である郵便とベンダーのインフラストラクチャを含む。1997年４月25日に発表された情報ベース証印プログラム鍵管理プラン仕様書は、ＵＳＰＳ製品/サービスプロバイダーとＰＳＤが使用する暗号鍵の生成、分配、使用、及び置換えについて明記する(ＩＢＩＰ　ＫＭＳ仕様書)。これらの仕様書は、まとめて「ＩＢＩＰ仕様書」といわれる。

ＩＢＩＰ仕様書は、独立型オープンメーターシステムについて定義し、ここではＰＣメーターという。ＰＣメーターは、プリンターが結合し、ホストシステム（ホストＰＣ）として作動するパーソナルコンピュータ(ＰＣ)に結合したＰＳＤを備える。ホストＰＣは、メータープリケーションソフトウェア及び対応するライブラリー(ここでは全体を「ホストアプリケーション」という)を実行し、１つ又はそれ以上の取り付けられてＰＳＤと通信する。ＰＣメーターは、ホストＰＣに接続したＰＳＤのみにアクセスできる。ＰＣメーターは、遠隔地のＰＳＤにアクセスすることはない。

ＰＣメーターは、ホストＰＣ上で、郵便料金分配、登録、再充填のための取引を処理する。処理は、ホストとそれに結合したＰＳＤの間で局内で行われる。例えば登録と再充填の取引のためにデータセンターへ接続することは、ホストから局内又はネットワークのモデム/インターネット接続を通じて局内で行われる。ＰＳＤへの借り方と貸し方の会計もまた、ホストＰＣ上に取引を記録して、局内で行われる。ホストＰＣは、例えば直列のポートごとに１つのＰＳＤをサポートする等、１つ以上のＰＳＤを収容しても良い。ワードプロセッサー、又は封筒デザイナー等のホストＰＣ上で実行される幾つかのアプリケーションプログラムは、ホストのアプリケーションにアクセスできる。

ＩＢＩＰ仕様書は、ネットワーク環境上のオープンメーターシステムを取り扱

わない。しかし、仕様書はこのようなネットワークベースのシステムを禁止してはいない。一般に、ネットワーク環境でネットワークサーバーＰＣは、ネットワーク上のクライアントＰＣに要請された遠隔の印刷を制御する。勿論、クライアントＰＣは、局内での印刷を制御する。

以下「仮想メーター」というネットワークメーターシステムの１つのバージョンでは、ＰＳＤが結合していない多くのＰＣを有する。ホストＰＣは、ホストのアプリケーションを実行するが、全てのＰＳＤ機能はデータセンターにあるサーバーで実行される。データセンターにおけるＰＳＤ機能は、データセンターにあるコンピュータに取り付けられた安全デバイスで実行することも、コンピュータ自体の中で実行することもできる。ホストＰＣは、郵便料金分配、メーター登録、メーター再充填等の取引を処理するためには、データセンターと接続しなければならない。取引はホストＰＣにより要請され、遠隔処理のためデータセンターへ送られる。取引はデータセンターで集中して処理され、結果はホストＰＣに戻される。資金の会計と取引の処理は、データセンターに集中する。例えば、本発明の譲受人に譲受けられた米国特許第5,454,038号、第4,873,645号を参照されたい。

仮想メーターは、ＩＢＩＰ仕様書の全ての現在の要求に適合するわけではない。特に、ＩＢＩＰ仕様書は、ＰＳＤ機能をデータセンターで実行するのを許可しない。しかし、各郵便利用者のＰＳＤがデータセンターにある仮想メーター構成により、ＩＢＩＰ仕様書で要求されるのと同等のレベルのセキュリティを提供できることが分かった。

従来のクローズドシステムの機械的電気的郵便料金メーターでは、印刷機能と会計機能の間に安全なリンクが要求された。１つの安全なボックス内で印刷と会計機能を実行するように構成された郵便料金メーターでは、安全ボックスの完全さは、メーターを周期的に調べることによりモニターされる。最近、デジタル印刷する郵便料金メーターは、メーター(会計)デバイスに結合したデジタルプリンターを備え、これをここでは郵便セキュリティデバイス（ＰＳＤ）という。デジタル印刷する郵便料金メーターにより、会計機構と印刷機構の間のリンクを暗号で安全保護することにより、物理的検査の必要性がなくなった。要するに、新

しいデジタル印刷郵便料金メーターは、ＰＳＤとプリントヘッドの間の安全な二地点間接続リンクを作成した。例えば、クリストファーB:ライトに発行され本発明の譲受人に譲受けられた米国特許第4,802,218号を参照されたい。安全なプリントヘッド通信の出来るデジタル印刷郵便料金メーターの例は、コネチカット州スタンフォードのピットニーボーズ社のパーソナルポストオフィス™である。

米国特許第4,837,645号、第5,454,083号では、郵便会計とトークンの生成が郵便料金証明プリンターから遠隔のデータセンターで行われる仮想メーターシステムと方法が開示されている。データセンターは安全な機構であるかもしれないが、会計とトークン生成の機能は郵便料金プリンターの局内の安全デバイスでは行われないので、ある固有のセキュリティの問題がある。仮想郵便料金メーターシステムは、安全保護されていないプリンター及び遠隔のデータのメーターシステムに結合したコンピュータを備える。郵便の会計とトークン生成は、データセンターで行われる。

データセンターは、ピットニーボーズ等のメーターのベンダー又は郵政公社の制御下にある集中化した機構である。このように、顧客がメーターを直接取扱う環境と比べて安全であると考えられる。しかし、データセンターに記憶したデータは、データセンターの要員によりアクセスできるので、少なくとも、このような要員による不注意による改変を受けることがある。データセンターに記憶されたユーザーとメーターデータの許可されない変化は、どのようなものでも仮想メーターシステムの完全さを損なう。

発明の開示

仮想郵便料金メーターシステムでは、従来の便料金支払いシステムでは得られない利点が得られる。郵便局にとって、仮想郵便料金メーターシステムは、全ての郵便料金の集中化した管理を行うことができる。別の利点は、郵便利用者がそれぞれ復元しなくても、直接各郵便物に対応付けられることである。郵便利用者には、メーターのハードウェア即ち郵便料金メーター又はＰＳＤは必要ではない。又、郵便利用者は、購入したＣＤ－ＲＯＭ等で有効な受信人の現在のリストを保持する必要はない。郵便利用者は、必要に応じて郵便の証印を得ることが出来る。最後に、メーターのベンダーは、物理的なメーターを追跡する必要はない。

仮想

郵便料金メーターシステムは、盗まれた又は再配置したメーターの問題をなくし、一般にメーター管理を簡単にする。

本発明は、仮想郵便料金メーターシステムのデータセンターにデジタルデータのセキュリティを提供し、データセンターに記憶したメーターとユーザーデータの偶然及び意図的な改変を防止する。本発明では、データセンターに記憶したメーターとユーザーの記録の許可されない修正を防止するため、セキュリティボックスを使用する。本発明は又、データセンターで行われる各郵便料金証明取引について、デジタルトークン生成プロセス及び対応する安全な会計の安全な制御を提供する。

仮想郵便料金メーターシステムのセキュリティの問題には、ユーザーの認証と、資金及び郵便料金取引と、メーターの記録とが含まれる。ユーザーの認証とメーターの記録のため、データベースは暗号鍵を普通テキストでなく暗号テキストで保持する。各取引について、時刻表示又は通し番号を含む取引を完全にするため使用される全てのデータは、デジタル署名され、署名は更新された取引記録として記憶される。このように取引記録を保持すると、記録が不注意で改変されることを防止する。

デジタル署名は合理的なセキュリティを提供するが、防弾ではない。「不正取引」等を検知するために、より頑強な検証を要するとき、履歴的に署名された記録を、現在の記録の代りに使用できることが分かった。本発明によれば、他のレベルのセキュリティが追加される。いったん署名が検証されると、取引データは、不注意又は意図的な不正取引の可能性を減らすため、フレッシュネスのチェックすることができる。

本発明では、郵便料金支払い証明のシステムと方法は、取引データに署名しメーターとユーザーの記録を検証するため、安全ボックスを使用する。このシステムと方法では、内部に複数のメーターの記録を記憶するデータベースを有するデータセンターが含まれる。各メーター記録は、郵便料金支払い証明を要求することを許可された複数の遠隔ユーザーデバイスに割り当てられたメーターの会計に

対応するメーター情報を含む。データセンターが郵便証印の要求を受取ると、データセンターの安全な双対プロセッサーが、適当なメーター記録を得て、メーター記録の署名を検証し、メーター記録のフレッシュネスデータを安全デバイスのフレッシュネスデータと比較することにより、メーター記録の認証を検証する。もし検証されれば、安全デバイスは次に、証明する郵便料金の価額を会計し、郵便料金支払い証明を生成し、メーター記録内のフレッシュネスデータを含むメーター情報を更新する。安全デバイスは次に、更新したメーター情報に署名し、署名をメーター記録内に記憶する。安全デバイスは次に、更新したメーター記録をデータベースに戻す。

図面の簡単な説明

上述した及びその他の本発明の目的と利点は、図面を参照して次の発明の詳細な説明を読めば、明らかであろう。図面において、同じ参照番号は同じ部分を表す。

図１は、郵便証印を分配する本発明の仮想郵便料金メーターシステムのブロック線図である。

図２は、図１の仮想郵便料金メーターシステムに使用する、データセンターのデータベースサーバーと安全ボックスのブロック線図である。

図３は、図１の仮想郵便料金メーターシステムにより郵便料金を証明するプロセスのフローチャートである。

図４は、図１の仮想郵便料金メーターシステムの安全メーターボックス内で実行されるプロセスのフローチャートである。

発明実施のための最良の形態

本発明を図面を参照して記述する。図１に、全体を10で示す仮想郵便料金メーターシステムを示す。仮想郵便料金メーターシステム10は、ゆうびん流斤を安全に証明するオープンシステムの証印を印刷する。仮想郵便料金メーターシステム10は、複数のパーソナルコンピュータ（ＰＣ）システム20（１つのみを示す）を備え、各ＰＣシステムは封筒又はラベルに郵便料金の証明を印刷するためプリンター22にアクセスできる。ＰＣ20は、郵便会計と郵便料金の証明を行う取引処理

のデータセンター30と接続されている。仮想郵便料金メーターシステム10により、各郵便利用者が、通常のＰＣを使用して、必要により郵便料金支払いの証明を遠隔で得ることができる。従来の郵便料金メーターシステムと異な

り、仮想郵便料金メーターシステム10は、郵便利用者のサイトにはメーターハードウェアがない。また、郵便資金も郵便利用者のサイトに保管されていない。全てのメーター機能と資金の会計は、ここで「メーター口座」という各郵便利用者の「郵便料金メーター」を表す機能的なソフトウェアとデータベース記録を使用して、データセンター30で行われる。

仮想郵便料金メーターシステム10の会計方法は、通常の前払い又は後払いシステムであってもよい。好適な方法は、各郵便利用者が最小限の金額を郵便利用者の仮想メーター口座に置く支払方法である。口座資金が特定のレベルより下に下がると、郵便利用者の口座に再充填される。仮想郵便料金メーターシステムに適する会計方法は、取引が行われるとき取引の価額が郵便利用者のクレジットカードに課金されるリアルタイム支払方法である。この方法はここでは「その都度課金」郵便料金支払いという。その理由は、郵便利用者が郵便物に印刷する準備が出来るまで、郵便利用者は郵便物の郵便料金を支払わないからである。

仮想郵便料金メーターシステムでは、ピットニーボーズ社等の「メーター」ベンダーは、郵便利用者にＰＣ20上で走るクライアントソフトウェアを提供する。クライアントソフトウェアは、ベンダーのインターネットサーバーからダウンロードしても良い。又は、クライアントソフトウェアは、ユーザーがデータセンター30との対話が出来るインターネットブラウザベースのホームページでも良い。メーターのベンダーは、またデータセンター30を管理する。クライアントソフトウェアは、１つの郵便物又は郵便物の束のための郵便料金を証明するためメーターの取引を行うデータセンター30との通信を開始する。好適な実施例では、クライアントソフトウェアは、データセンターへの接続を確立し、各郵便物の郵便料金の価額、受信人情報、（オプションで）差出地等の要求する取引に関する郵便情報を提供することにより、郵便の証印を要求する。データセンター30は、郵便情報を受取り、郵便物の差出地ジップコードを求め、会計機能を行い、トークン

又はデジタル署名等の郵便料金支払いの暗号化した証明を生成し、トークンを含む証印情報をＰＣ20へ送る。ＰＣ20は、証印の情報を受取り、証印のビットマップを生成し、このビットマップをＰＣのモニター（図示せず）に表示し、またプリンター22により郵便物に印刷することができる。ＰＣ20は次に、データセンター30との接続を切るか、又は他の取引を要求する。ＰＣ20とデータセンター30との接続は、インターネット上のネットワークサービスプロバイダー経由で、又はＰＣのモデムを使用して直接ダイアルしても良い。

仮想郵便料金メーターシステム10は、各郵便利用者のサイトで従来のメーターデバイスを保持し会計する必要性をなくし、各郵便利用者による複数の差出地からの要求を取り扱う柔軟性を与える。仮想郵便料金メーターシステム10はまた、リアルタイムアドレス指定のウィルス予防、直接マーケッティングサービス、その都度課金する郵便料金支払い等の従来のメーターデバイスでは得られない価値が高まるサービスを提供する。仮想郵便料金メーターシステム10は、データセンター30によるユーザー認証を提供し、有効な口座を有する郵便利用者を識別する。各要求について郵便利用者が、ユーザーの名前、パスワード又は他の通常の方法等で認証されたとき、データセンター30は要求を聞き、証印情報をＰＣ20へ戻し、そこで証印が生成され、郵便物に印刷される。

図１に戻ると、郵便利用者は、ＰＣ20でクライアントソフトウェアを走らせることにより、郵便料金証明取引を開始し、ＰＣ20はデータセンター30にコンタクトする。データセンター30で、通信サーバー32が、色々の通信技術とプロトコルからの連結性を支援する。通信サーバーは、全ての入力するトラフィックを併合し、機能サーバー34に向ける。機能サーバー34は、郵便利用者のサインオン、郵便料金分配、郵便報告を支援するアプリケーションソフトウェアを含む。全ての郵便利用者とメーターの情報は、データベースサーバー36からアクセスすることができる。データベースサーバー36には、後述するように、安全な暗号プロセスとプロトコルを使用して情報が安全保護されて記憶されている。データセンター30は、データベースサーバー36の各メーター口座の暗号鍵を保持する。暗号鍵は、郵便料金の証明と検証のために使用され、又データベースサーバー36に記憶さ

れる記録のセキュリティのために使用される。鍵管理システム38が、仮想郵便料金メーターシステム10で使用される全ての暗号鍵を管理する。暗号鍵は、遠隔の位置で検証するため分配することも出来る。1995年10月23日出願で本発明の譲受人に譲受けられた米国特許出願第08／553812号は、このような鍵管理システムを記述する。

郵便利用者は、データセンター30とのオンラインサインアッププロセスにより、メーターの口座を設立することができる。サインアップの間、郵便利用者はＰＣ20でユーザーの名前、パスワード、支払方法等の口座情報を入力する。登録費用はこの時課金することができる。データセンター30は、ピットニーボーズ社等のメーターのベンダーにより管理されるのが好ましいが、全てのメーターのライセンス及び郵便利用者と郵便局の間の契約を取り決める。

本発明では、ＰＳＤは存在しない、即ち郵便料金支払いを要求するＰＣに結合したメーターデバイスはない。仮想郵便料金メーターシステム10は、ＰＳＤの会計とメーター機能をＰＣ20のメーターソフトウェアとデータセンター30で実行され更新される郵便利用者の会計情報で置き換える。仮想郵便料金メーターシステム10は、各郵便利用者に、複数の投函元から取引を開始できる能力を有するメーターシステムを提供する。例えば、前述した国際特許出願番号［代理人番号E-735を参照されたい。

要求された取引の投函元を求めるには幾つかの方法を使用することができる。例えば、電話でかける人のＩＤを使用する差出地ジップコードを求める方法は、1996年12月31日出願で本発明の譲受人に譲受けられた来国特許出願第08/775,818号に開示されていて、その出願をここに参照する。

本発明によれば、ここでは安全「ボックス」という１つ又はそれ以上の暗号モジュールが、データセンター30内にあり、暗号化プロセスを実行するため使用される。各安全ボックスは、安全で、不正がはっきり分かり、不正に応答するプロセッサーとメモリーを含むデバイスであり、暗号鍵を記憶し、デバイスの安全境界内の鍵を使用して暗号オペレーションを実行する。データセンター30は、後述する幾つかの種類の安全ボックスを有する。好適な実施例では、データセンター

30は冗長と性能のため各種類の複数のボックスを備える。

鍵管理システム38は、各安全ボックスを相互にシードするため、ランダム数を生成するのに使用するトップレベルの鍵を提供する製造ボックス（図示せず）を有する。共通の暗号鍵を居有することにより、安全ボックスは、データセンター30内で安全に通信する。鍵管理システム38はまた、メーターボックス44（後述する）と共通鍵を共用する「スチール」ボックス（図示せず）を備え、各メーターの口座のための郵便料金証明取引のためのマスタートークンを暗号化／復号化する。各スチールボックスは、ベンダー鍵と郵便鍵を暗号テキストの１つの記録に併合する。各メーターの口座のため、データセンター30は、ベンダーと郵便の鍵を使用してトークン鍵を作成し、メーターの登録（昇順と降順）と、メーターのフレッシュネスデータ（後述する）と、メーター記録の一部としての他の郵便情報とを初期化し、メーター記録をデータベースサーバー36に記憶することにより、データベースサーバー36内にロジカルメーター即ちメーター記録を作成する。

データセンター30はまた、メーター記録内で暗号化されたトークン鍵を復号化するため、スチールボックスと秘密鍵を共有するメーターボックス44を備える。メーターボックス44はまた、データベースサーバー36で記憶される取引記録のデジタル署名に使用される鍵を保持する。メーターボックス44に記憶される他の情報は、メーターボックス44により処理される各メーター記録のためのフレッシュネスデータである。各郵便料金取引について、メーターボックス44は少なくとも１つのデジタルトークンを生成し、又は郵便取引に署名し、取引に対応するメーター記録を更新する。データベースサーバー36内の各メーター記録は、郵便資金と暗号テキストのトークン鍵を含む。メーターボックス44は、トークン鍵を使用して、トークンを生成し、メーター記録の郵便資金を更新し、更新されたメーター記録に署名する。このように、メーターボックス44は各取引の安全な会計を実行し制御する。メーターボックス44はまた、トークン又は取引署名を検証するのに使用し、取引のため郵便料金証明の検証をすることができる。

データセンター30はまた、スチールボックスと別の秘密鍵を共用する認証ボッ

クス40を備え、データベースサーバー36の暗号テキストに記憶されたユーザー認証鍵を復号する。認証ボックス40はまた、復号化した認証鍵を使用して認証アルゴリズムを実行して、郵便利用者を認証する。この機能を鍵管理システム38のスチールボックスに追加し、データセンター30に別体のボックスの必要性をなくすことができる。

最後に、データセンター30は、スチールボックスと他の秘密鍵を共用する取引ボックス42を備え、メーターボックス44により署名されたメーター記録以外のユーザー取引記録、例えばログインとログイン履歴記録等に署名する。取引ボックス42は、後に次の取引が要求されたときに、取引記録の署名を検証する。

図２は、メーターデータベース60、郵便利用者データベース62、メーター記録のデータベース64を含むデータベースサーバー36の構成を示す。メーターデータベース60は、メーター通し番号、記録更新カウンター、昇順レジスター、降順レジスター、他の郵便の値等、各メーターの口座と対応するメーター情報を備える。メーターデータベース60はまた、メーターボックス44により署名された取引記録の記憶装置を含む。取引記録は、例えば、差出地郵便コード、取引日／時刻、証印データ、配達地郵便コード、トークン、郵便価額、デジタル署名を備える。郵便利用者データベース62は、郵便利用者情報と、郵便利用者をメーターの口座と組合せる情報を備える。

動作において、通信サーバー32は、郵便利用者のＰＳ20からメーター取引の要求を受取る。機能サーバー34内のアプリケーションソフトウェアが、取引要求の処理を制御する。機能サーバー34は郵便利用者データベース62とメーターデータベース60にアクセスし、要求を開始する郵便利用者のメーター口座に対応する、適当なメーター記録64を含む記録を得る。機能サーバー34は、郵便利用者データベース62から認証ボックス40へ郵便利用者記録を通信し、次に認証ボックス40が、取引を要求する郵便利用者を認証する。いったん、郵便利用者が認証されると、機能サーバー34は、適当なメーター記録64をメーターボックス44へ通信し、メーターボックス44が、記録のため署名とフレッシュネスデータを検証する。メーターボックス44は、メーター記録64内の記憶された暗号鍵を復号化し、メーター

記録64の昇順及び降順レジスターで会計機能を実行し、鍵を使用して要求された取引のためのトークンを生成する。次にメーターボックス44は、証印のためのデータを生成し、メーター記録64を止める。次に、更新され署名された記録は、データベースサーバー36へ戻され、そこでメーターデータベース60の一部として記憶される。

データセンター30では、認証鍵は普通テキストでは得られないが、郵便利用者に分配しなければならない。各郵便利用者に認証鍵を分配し更新する通常の方法を使用することが出来る。例えば、前述の米国特許出願第08／553,812号を参照すると、安全ボックスと郵便利用者のＰＣへ暗号鍵を分配し更新する鍵管理システムが記述されている。

鍵管理システム38の１つの重要なタスクは、郵便鍵を得て、それをベンダーの鍵と組合せることである。鍵管理システム38で、スチールボックスは、各メーターの口座のため、１つのメーター記録64内にメーターの通し番号（製造番号）を作成し、またベンダーと郵便の鍵を作成する。

暗号化／復号化アルゴリズムでは、暗号化鍵を暗号化するため１組のトリプルＤＥＳ鍵を使用し、証印のためのトークン即ち署名を生成する。トリプルＤＥＳ鍵の他の組は、メーター記録に署名するため使用される。メーターボックス44は、トリプルＤＥＳ鍵の両方の組を安全に保管する。証印のトークン即ち署名を生成するメーター鍵の全部の組を暗号化するのに１つだけの鍵を使用することがないようにするため、導出した鍵が使用される。トリプルＤＥＳ鍵の第１の組は、各メーター記録のメーター（口座）通し番号を暗号化することにより、トリプルＤＥＳ鍵を導出する。次に導出したトリプルＤＥＳ鍵が、証印の暗号化鍵を暗号化し、それをデータベースサーバー36に記憶する。署名のためのトリプルＤＥＳ鍵の第２の組は、同様に署名鍵を導出するのに同様の方式を使用する、即ち、鍵を導出するのにメーターの通し番号をデータとして使用する。両方の目的のため、１組のトリプルＤＥＳ鍵を使用することもできる。しかし、各鍵の組は、１つの目的のみに使用するのが好ましい。

本発明の好適な実施例では、メーター記録、郵便料金取引、資金移転記録、マ

スター口座記録等、デジタル署名を要する全ての取引と記録に署名するのに１つの共通鍵を使用する。各ボックスの複数のボックスは、冗長のため、また取引の数が大きくなると作業負荷を分担するため使用される。メーターボックス44又は認証ボックス40等の署名ボックスもまた、記録の署名を検証する。

メーター記録64のための署名アルゴリズムに関して、メッセージ認証コード（ＭＡＣ）を使用して、感度の良い仮想郵便料金メーター10記録のため、メッセージの完全さを提供する。このＭＡＣは、データ暗号化規格（ＤＥＳ）の複数のアプリケーションを含む。証明鍵は、現在の月又は年を使用して更新される。

製造中に、２つの初期のマスター鍵がメーターボックス44の不揮発性メモリー（ＮＶＭ）に入力される。ＮＶＭは、永久保管のため、また鍵情報への外部アクセスを防止するため使用される。証印のための鍵と署名のための鍵は、後述するように従来の方法で導出される。仮想郵便料金メーター10の記録署名検証アルゴリズムは、単にメーター記録64内の署名アルゴリズムとデータを使用してメーター記録64の署名を再計算し、計算した署名をメーター記録64内の署名と比較するだけである。

図３に、仮想郵便料金メーターシステムで郵便証明取引を安全に実行するプロセスを示す。ステップ100で、通信サーバー32が、郵便利用者のＰＣ20から郵便料金証明の要求を受取る。ステップ105で、機能サーバー34が、データベースサーバー36に記憶されている郵便利用者の口座情報へのアクセスを要求する。ステップ110で、データベースサーバー36は、郵便利用者情報、要求を開始する郵便利用者に対応するメーター記録を含むメーター情報を送る。ステップ115で、機能サーバー34は、郵便利用者情報を認証ボックス40へ送る。ステップ120で郵便利用者が認証されると、次にステップ125で、機能サーバー34はメーター記録を含むメーター情報をメーターボックス44へ送る。ステップ130で、メーターボックス44は、メーター記録を認証し、記録の一部である暗号化されたトークン鍵を復号化し、記録のフレッシュネスを検証し、会計を実行し、トークンを生成し、フレッシュネスデータを更新し、メーター記録に署名し、それが機能サーバー34へ戻される。ステップ135で、機能サーバー34は更新し署名したメーター記録を

データベースサーバー36へ送り、トークン及び証印を作成するのに必要な対応する郵便情報を通信サーバー32へ送る。ステップ140で、データベースサーバー36は、更新し署名したメーター記録を記憶する。ステップ145で、通信サーバー32はトークンと郵便情報を郵便利用者のＰＣ20へ送る。

図４に、仮想郵便料金メーターシステムの安全メーターボックス内で実行されるプロセスを記述する。ステップ200で、メーターボックス44が署名したメーター記録を受取る。ステップ205で、メーター記録の署名が検証される。ステップ210で検証されなければ、ステップ215で、メーターボックスは取引を終了させ、機能サーバー34に不正の可能性があると警告する。もし署名が検証されれ

ば、ステップ220で、メーターボックスは、各メーターの口座についてメーターボックスに記憶されたフレッシュネスデータを、メーター記録の一部として記憶されたフレッシュネスデータと比較する。子の比較のために選択されるフレッシュネスデータは、各取引に独自のデータでなければならない。好適な実施例では、記録更新カウンターが使用されるが、ランダム数、時刻表示、又は他のその時限りの値を使用することもできる。ステップ220での比較により、仮想郵便料金メーター取引の間、不注意又は意図的に旧メーター記録を現在のメーター記録で置き換えることを防止する。

ステップ225で、比較したフレッシュネスデータが等しくなければ、ステップ230で、メーターボックスは取引を終了させ、機能サーバー34に不正の可能性があると警告する。もしメーター記録に記憶したフレッシュネスデータがメーターボックスに記憶したメーター記録に対応するフレッシュネスデータと等しければ、次にステップ235で、メーターボックスは、メーター記録の一部として暗号化した形式で受取ったトークン鍵を復号化する。ステップ240で、メーターボックスは、取引のための会計機能を実行する。例えば、昇順レジスターをインクリメントし、降順レジスターをディクレメントし、記録更新カウンターをインクレメントする。ステップ245で、メーター記録のフレッシュネスデータが更新される。ステップ250で、メーターボックス44に記憶したフレッシュネスデータが更新される。ステップ255で、メーターボックスは暗号化したトークン鍵を使用してト

ークンを生成する。ステップ260で、メーターボックスは、メーター記録に新しい登録値と記録更新カウンターを記憶することにより、メーター記録を更新し、次にメーターボックスに記憶した鍵を使用して更新された記録に署名する。ステップ265で、メーターボックスは、更新し署名したメーター記録をデータベースサーバー36へ送り、これはメーター記録に割り当てられる次のメーター口座の取引まで保管される。

本発明の実施例は、郵便料金メーターシステムとして記述したが、本発明は、金銭取引、項目取引、情報取引等の取引証明を含むどのような価値のメーターシステムにも適用することが出来る。

本発明は、特定の実施例に関連して記載した。しかし、前述したように、秘密鍵の代りに公開鍵を使用する等の変更を行うことができる。従って、特許請求の範囲は、本発明の精神と範囲に入る変形を包含することを意図している。

【図１】

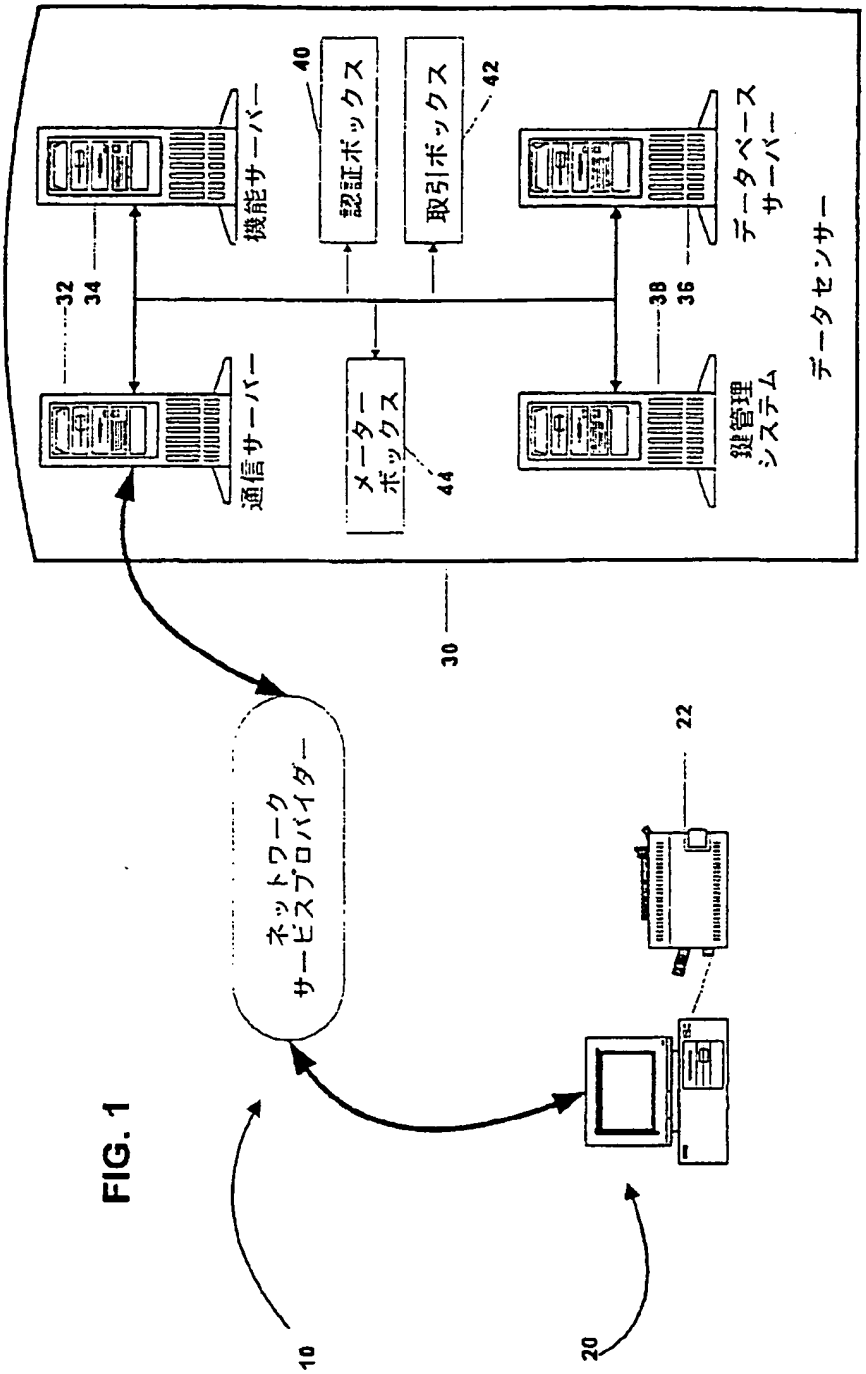
データセンサー
機能サーバー
認証ボックス
40
取引ボックス
42
データベース
サーバー
32
34
38
36
通信サーバー
メーター
ボックス
44
鍵管理
システム
30
ネットワーク
サービスプロバイダー
22
10
20

FIG. 1

【図２】

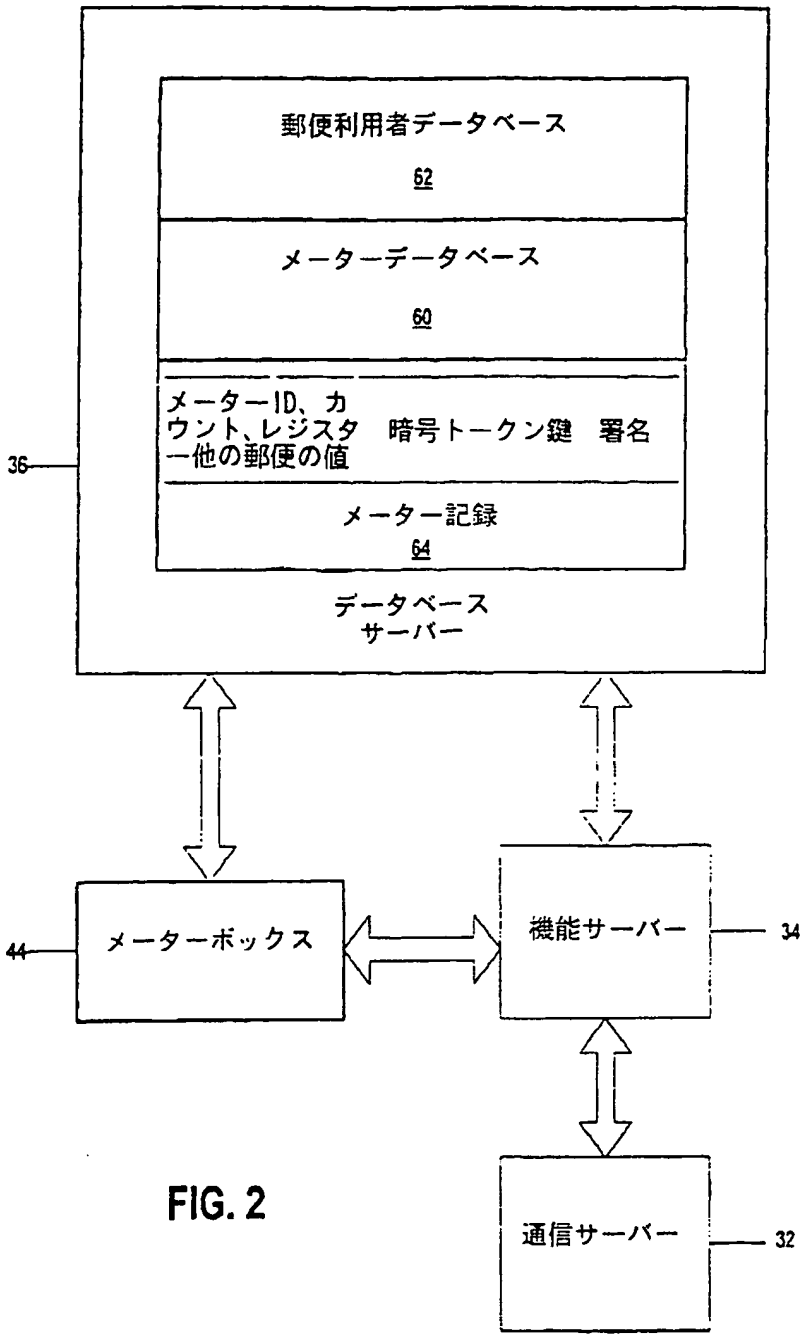
郵便利用者データベース
62
メーターデータベース
60
メーターID、カウント、レジスタ一他の郵便の値
暗号トークン鍵
署名
メーター記録
64
データベースサーバー
36
メーターボックス
44
機能サーバー
34
通信サーバー
32

FIG. 2

【図3】

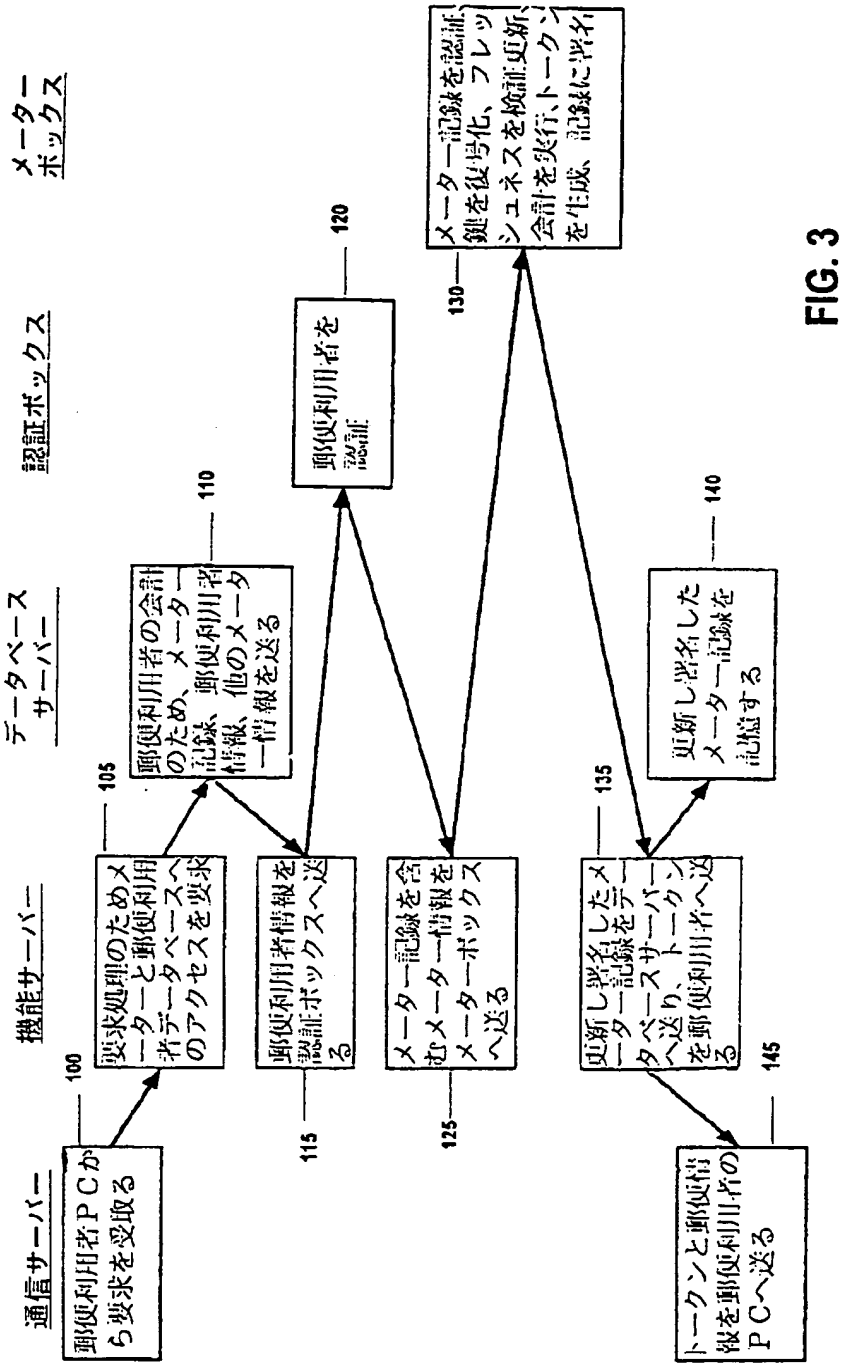
通信サーバー
機能サーバー
データベースサーバー
認証ボックス
メーターボックス
郵便利用者PCから要求を受取る
100
要求処理のためメーターと郵便利用者データベースへのアクセスを要求
105
郵便利用者の会計のため、メーター記録、郵便利用者情報、他のメーター情報を送る
110
郵便利用者を認証
120
メーター記録を認証鍵を復号化、フレッシュネスを検証更新会計を実行、トークンを生成、記録に署名
130
郵便利用者情報を認証ボックスへ送る
115
メーター記録を含むメーターボックスへ送る
125
更新し署名したメーター記録をデータベースサーバーへ送り、トークンを郵便利用者へ送る
135
更新し署名したメーター記録を記憶する
140
トークンと郵便利用者情報を郵便利用者のPCへ送る
145

FIG. 3

【図４】

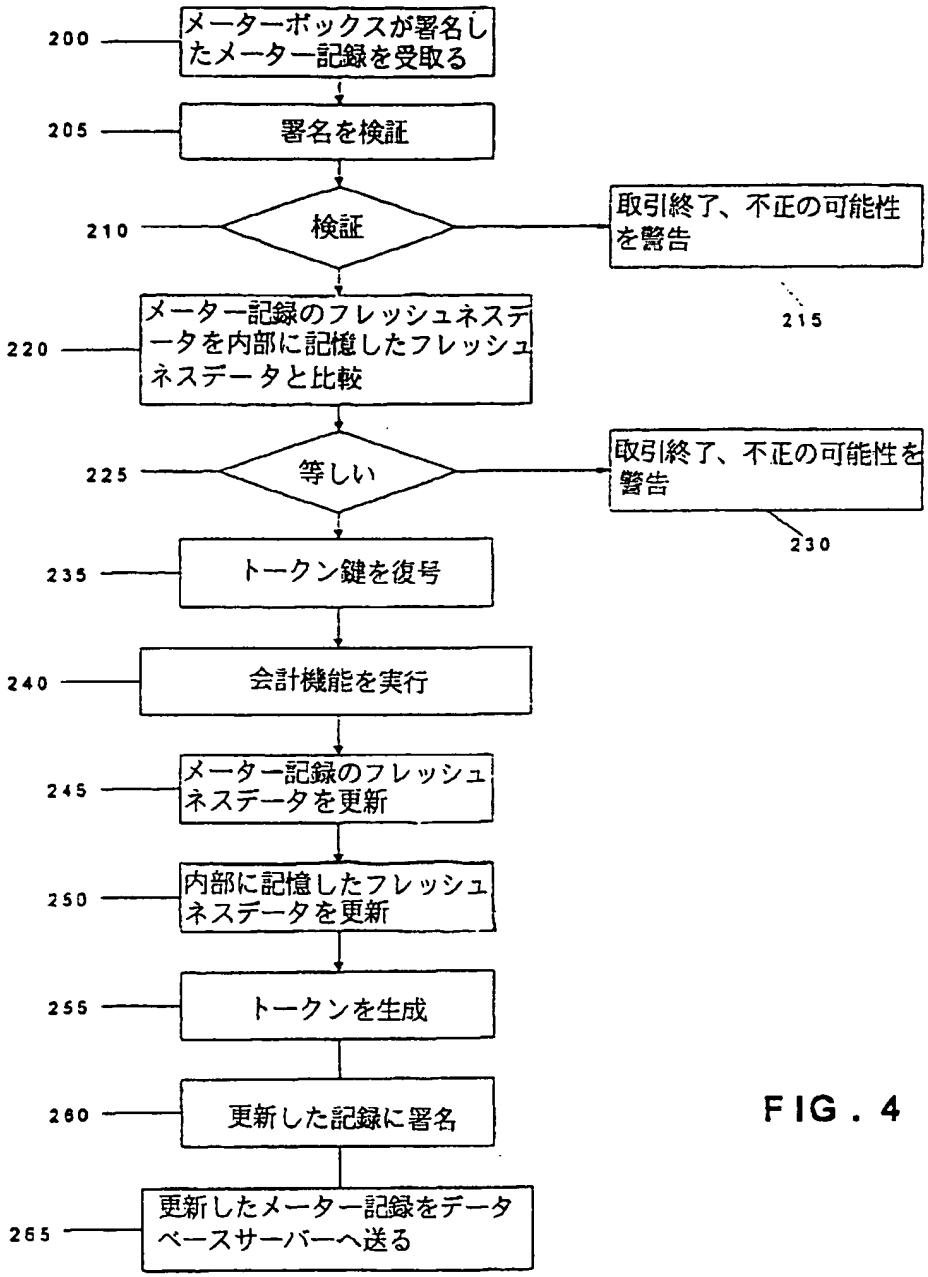
200
メーターボックスが署名したメーター記録を受取る
205
署名を検証
210
検証
取引終了、不正の可能性を警告
215
220
メーター記録のフレッシュネスデータを内部に記憶したフレッシュネスデータと比較
225
等しい
取引終了、不正の可能性を警告
230
235
トークン鍵を復号
240
会計機能を実行
245
メーター記録のフレッシュネスデータを更新
250
内部に記憶したフレッシュネスデータを更新
255
トークンを生成
260
更新した記録に署名
265
更新したメーター記録をデータベースサーバーへ送る

FIG. 4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/12276

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G07B 17/00
US CL :705/401; 340/825.35; 395/200.33
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 235/3811; 340/825.35; 395/200.33, 200.47; 705/401, 408, 410

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
NONE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,376,299 A (RIVEST) 08 March 1983, see abstract.	1-13
A	US 4,567,359 A (LOCKWOOD) 28 January 1986, see abstract.	1-13
A	US 4,757,537 A (EDELMANN et al) 12 July 1988, see abstract.	1-13
A	US 4,775,246 A (EDELMANN et al) 04 October 1988, see abstract.	1-13
A	US 4,802,218 A (WRIGHT et al) 31 January 1989, see abstract.	1-13
A	US 4,873,645 A (HUNTER et al) 10 October 1989, see abstract.	1-13

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 24 AUGUST 1998	Date of mailing of the international search report 28 SEP 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer EDWARD R. COSIMANO Telephone No. (703) 308-9783

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/12276

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,454,038 A (CORDERY et al) 26 September 1995, see abstract.	1-13
A, E	US 5,781,438 A (LEE et al) 14 July 1998, see abstract.	1-13

Form PCT/ISA/210 (continuation of second sheet)(July 1992)*

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), AL, AM, AU, AZ, BA, BB, BG, BR, BY, CA, CN, CU, CZ, EE, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, RO, RU, SD, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW

(72)発明者 ヘインデン ゲアリー エム
アメリカ合衆国 コネチカット州 06484
シェルトン ウッドセンド アベニュー 14

(72)発明者 リー ディヴィッド ケイ
アメリカ合衆国 コネチカット州 06468
モンロー アルパイン ロード 12